Red Hat Linux 6.X als een Internet Gateway voor een Thuis Netwerk

Paul Ramsey
Vertaler: *Reggy Ekkebus, reggy@zeelandnet.nl* January 22, 2000

Dit is een simpel document over hoe een pc te configureren met Red Hat 6.X en aanverwante Linux varianten voor het maken van een internet gateway voor een thuis Netwerk. Dit document bevat ook masquerading, DNS, DHCP, en basisveiligheid.

Inhoudsopgave

1 Introductie

Deze pagina bevat een simpele beschrijving van hoe een Redhat 6.X te configureren als een internet gateway voor thuis of een klein bedrijfje. De instructies zijn erg simpel: speciale gevallen worden hier niet behandeld, en sommige stelling over hoe netwerkadressen gebruikt worden. De belangrijkste stellingen zijn:

- Je hebt een Kabel of ADSL connectie naar het Internet.
- Je kan *Red Hat 6.X* installeren op een van je computers. Deze richting is ook van toepassing op RedHat afgeleiden, zoals *Mandrake 6.X* welke wordt gedistubieerd door MacMillan Publishing onder verschillende labels.
- Je Linux computer heeft twee met Linux compatible netwerkkaarten
- Als je meer dan twee computers hebt dan heb je ook een hub nodig of een cross-link kabel niet meer dan twee computers hebt.
- Je weet hoe je text moet editten onder Linux.
- Je kan als `root` inloggen op je machine. Je weet hoe je RPM's moet installeren van je Linux cdrom.

Als je van boven staande niets weet weet, dan is het waarschijnlijk dat dit document niets voor je is.

Tijdens het installatie proces is er niets specials te doen. Kies simpel een installatie waarvan je denkt dat ie bij je past. Dit document geeft aanwijzingen om alles te installeren wat nodig is om een thuis netwerk te maken, om te voorkomen dat je stellingen maakt over wat geinstalleerd of geconfigureerd is tijdens de installatie. Om zeker te weten dat dingen werken en er geen misverstanden zijn over waar informatie naar toe gaat, alle configuratie wordt gedaan door het direct editten van de configuratie files in tegenstelling tot het gebruiken van een GUI configuratie tool dat bij Red Hat zit. Aan de ene kant zal dit een beetje moeilijker zijn dan het moet zijn; maar aan de andere, zal je je beter kunnen over brengen naar een andere distributie of situatie (zoals, wat als X het niet doet, of als je een server zonder monitor installeert).

1.1 Versies

De laatste versie van dit document is altijd te vinden op *http://www.coastnet.com/˜pramsey/linux/homenet.html* voor de HTML versie en *http://www.coastnet.com/˜pramsey/linux/homenet.sgml* voor de SGML versie.

- December 21, 1999 : Eerste versie.
- Januari 2, 2000 : Suggestie van John Mellor over het opzetten van externe netwerk gewoonte's.
- Januari 22, 2000 : Een kleine update over identieke netwerk kaarten en info over IP aliasing van Chris Lea.

1.2 Copyright

- De copyright mededeling hier boven en de permissie notitie moeten compleet behouden blijven, op alle komplete of stukjes kopie's
- Elke vertaling of afgeleid werk moet bij de auteur worden aangevraagd voor dat deze gedistribueerd wordt.
- Als je werk in delen distributeerd, moet het een instructie bevatten hoe je aan de complete manual kunt komen.
- Een klein deel mag gereprduceerd worden als illustratie voor een overzicht of noteringen in ander werk zonder deze permissie mededeling als een goed citaat is gegeven.

Uitzonderingen op deze regels mogen worden gegeven voor school doeleinden: Vraag het aan de auteur. Deze beperkingen hier zijn om ons de auteurs te beschermen, niet om beperkingen op te leggen voor degenen die het willen leren of uitdragen

2 Aansluiten van de Hardware

Afhankelijk van of je een hub gebruikt of niet, je netwerk structuur zal weinig anders zijn. Ik behandel enkel netwerken met RJ45 bekabeling (dat spul dat lijkt op telefoon kabels) dus geen coax bekabeling. Met coax kan je veel machines aan elkaar koppelen zonder een hub, maar je moet voorzichtig zijn met het termineren van connecties enzo. Als je al een klein beetje van netwerken weet dan is deze uitleg groten deels dubbel.

2.1 Met een Hub

Als je een hub hebt, dan zou je netwerk er *zo* `<http://www.coastnet.com/~pramsey/linux/w_hub.gif>` uit kunnen zien.

Verbind de `eth0` kaart op de Linux computer met de kabel modem of ADSL box door gebruik van de kabel bijgeleverd door de service provider tijdens de installatie (of een waarvan je weet dat die werkt in die configuratie. Dit is belangrijk omdat soms kabel modems graag crossover verbonden willen worden en soms rechtdoor: de kabel die het bedrijf je heeft gegeven is de kabel die je moet gebruiken.

Verbind de `eth1` kaart in de Linux computer met de hub met een rechtdoor kabel. Verbind alle andere computers met de hub doormiddel van en rechtdoor kabel.

2.2 Zonder een Hub

Als je geen hub hebt, kun je nog steeds een computer verbinden met je Linux doos, met een crossover kabel. Je topologie ziet er dan *zo* `<http://www.coastnet.com/~pramsey/linux/wo_hub.gif>` uit.

Verbind de `eth0` kaart in de Linux box met de kabel modem of ADSL box door het gebruik van de kabel geleverd door de service provider. Verbind de `eth1` kaart in de Linux box met de andere computer doormiddel van een crossover kabel.

2.3 Met maar een Netwerk kaart

Dit is niet een aanteraden configuratie (in deze configuratie zijn je interne en externe netwerk op het zelfde fisieke adres, en zijn daardoor theoretisch gezien gevoeliger voor een kraak; in werkelijk heid, is het risico erg laag), maar het *kan*. Je kan er van denken wet je wil.

De Linux kernel bied ondersteuning voor "IP aliasing", wat een ethernet kaart instaat stelt om twee verschillende IP adressen gelijkertijd te gebruiken. De standaard kernel die bij Red Hat en Mandrake zitten hebben ondersteuning voor IP aliasing standaard. Om je gateway in te stellen met maar een netwerk kaart, in alle volgende code voorbeelden gewoon de `eth1` met `eth0:0` vervangen.

In een enkele kaart situatie is een DHCP server draaien niet aan te raden.

Plug al je machines en je kabel modem of ADSL box in de hub. Kruis je vingers en ga door.

3 Het netwerk configureren

Ok, nu heb je Linux geinstalleerd op je gateway computer. Je kan zelfs al een van je netwerk kaarten geconfigureerd hebben, en verbinding met het internet ingesteld hebben. Hoewel, we beginnen vanaf het begin en gaan ervan uit dat er nog niets is geconfigureerd.

Log in als `root`. Alle instructies gegeven in die document nemen aan dat je ingelogd bent als root.

De Linux kernel verwijst naar je twee netwerk kaarten als `eth0` en `eth1`, dus dat is hoe ik naar ze ga verwijzen van nu af aan. Het probleem is, welke is welke? Hier is een "simpele" manier om het uit te vinden, gegarandeerd om op z'n minst voor 50% van de keren te werken. Leg je computer op de tafel het moederbord horizontaal en de achterkant naar je toe (net alsof je er iets aan gaat doen). De meest linker kaar is `eth0` – je kan het markeren met een beetje tape. Schrijf nu de fabrikant en het model van beiden op een stuk papier.

Ok laten we kijken of `eth0` en `eth1` automatisch herkent worden door de kernel. Type `ifconfig eth0` en `ifconfig eth1`. In beide gevallen, als de kernel je kaart heeft herkent, zie je iets als dit (het maakt niet uit dat de cijfertjes een beetje anders zijn):

```
eth0   Link encap: Ethernet   HWaddr 00:60:67:4A:02:0A
       inet addr:0.0.0.0  Bcast:0.0.0.0  Mask:255.255.255.255
       UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
       RX packets:466 errors:0 dropped:0 overruns:0 frame:0
       TX packets:448 errors:0 dropped:0 overruns:0 carrier:0
       collisions:85 txqueuelen:100
       Interrupt:10 Base address:0xe400
```

Als je kernel de netwerk kaart niet herkent zul je iets als dit zien:

```
eth0: error fetching interface information: Device not found.
```

3.1 Een netwerk driver configureren

Als beide netwerk kaarten zijn gevonden, ga dan naar de volgende sectie. Zoniet lees dan deze sectie.

OK, dus een of beide kaarten worden niet herkent door de kernel. Dit is geen probleem, echt. Wat we moeten doen is de kernel iets precieser vertellen waar hij de kaarten kan vinden. Er zijn een helehoop bochten en draaien, ik ga ze niet allemaal vertellen. Onthoud, als het echt niet gaat kijk dan in de *Ethernet HOWTO*. Hier kun je veel adviesen vinden.

- *Je hebt een PCI netwerk kaart.* Je zit waarschijnlijk goed, aannemend dat het niet supernieuw en exclusief is dat er geen driver voor is. Je kan meestal veel vinden over je netwerk kaarten (en andere dingen) door het lezen van `/proc/pci` en het opschrijven van merk en model.

- *Je hebt een ISA netwerk kaart.* Het is mogelijk dat je het IO base adres en het IRQ van de kaart moet weten. Je hebt handleidingen, toch? Zo niet, dan is dit het goede moment om naar de site van de maker te gaan en kijk of zij online informatie hebben. Of als je een oude DOS configuratie diskette hebt, boot dan DOS en kijk of er een setup programma is dat het adress en IRQ leest en schrijft.
- *Je hebt een ISA Plug'n'Play kaart.* Je moet eerst leren hoe je het moet configureren – Lees de *Plug'n'Play HOWTO*. Gelukkig, als je de kaart hebt geconfigureerd weet je precies het IO adres en het IRQ.

Nu je weet wat het model en merk van de `eth0` en `eth1` is kan je naar de *compativiliteits pagina* gaan van de *Ethernet HOWTO* om te kijken of je kaart erbij staat. Kijk naar de aanbevolen driver, en de informatie over een speciale driver die je kaart misschien nodig heeft. Schrijf het op.

Het is tijd om een configuratie file aan te passen! De file die we gaan aan passen is `/etc/conf.modules`. Open deze file in de text editor naar keuze. Omdat er zo veel mogelijke manieren en combinaties van dingen zijn om in de file te komen, ga ik mijn eigen gateway als voorbeeld gebruiken. Ik heb een PCI 10/100MB kaart gebaseerd op de VIA Rhine chip, en een plain-jane 10MB NE2000 kloon. Ik gebruik de 100MB kaart voor het interne netwerk en de 10MB kaart voor het externe netwerk. Mijn `/etc/conf.modules` file ziet er zo uit:

```
alias parport_lowlevel parport_pc
alias eth0 ne
options ne io=0x300 irq=10
alias eth1 via-rhine
```

Mijn `conf.modules` file is zo uitgelegd:

- De eerste regel staat er om mijn paralelle poort om te printen te configureren. Je hebt waarschijnlijk dezelfde regel. Laat deze regel met rust.
- De tweede regel (`alias eth0 ne`) verteld de kernel om de ne driver te gebruiken voor het `eth0` device.
- De derde regel (`options ne io=0x300 irq=10`) verteld de ne driver op welk io adres en irq hij de ISA kaart zal vinden. Als je een ISA kaart hebt zal je waarschijnlijk zo iets dergelijks moeten gebruiken, verander gewoon de driver naam en de io en irq informatie voor je kaart.
- De vierde regel `alias eth1 via-rhine`) verteld de kernel dat hij de via-rhine driver voor `eth1` moet gebruiken. Omdat mijn `eth1` kaar een PCI kaart is, moet ik geen io en irq informatie meegeven: het PCI subsysteem configureert de kaart automatisch.

Je kan kijken in de `conf.modules` om te kijken of de alias regels goed zijn ingesteld voor beide kaarten, en de goede optie regels voor al je ISA kaarten. Je kan al regels hebben in je `conf.modules` voor elke ethernet kaart die je hebt geconfigureerd tijdens de installatie.

Als je klaar bent met het editten van de `conf.modules`, probeer dan `ifconfig eth0` en `ifconfig eth1` opnieuw. Je kan enkele waarschuwingen en fouten krijgen als je met de IO adressen en IRQ's speelt zonder een boekje van de fabriek.

3.1.1 Twee identieke netwerk kaarten

Dus, je was erg slim, je hebt twee identieke netwerk kaarten gekocht voor je Linux gateway en nu kun je ze niet samen laten werken? Maak je geen zorgen, om ze goed te laten werken is gewoon de goede syntaxis gebruiken in /etc/conf.modules. Bijvoorbeeld, het IO en IRQ nummer zijn ingesteld, en ik ga er van uit dat je twee dezelfde NE2000 clones hebt gekocht (een gewone keuze). Dan ziet je /etc/conf.modules file er zo uit:

```
alias eth0 ne
alias eth1 ne
options ne io=0x330,0x360 irq=7,9
```

De adres opties zijn allemaal gegeven op de zelfde regel, en het eerste nummen voor elke adres type is voor de eth0, en het tweede voor eth1.

3.2 Het binnen netwerk configureren

Het "binnen netwerk" is het netwerk waar al je thuis/kantoor machines op willen zitten. Het "buiten netwerk" is een het grote angstaanjagende internet aan de andere kant van je Linux box. Het binnen netwerk is compleet afgeschemd van het buiten netwerk door de Linux box, wat als een gemiddelde sterke firewall dient.

3.2.1 Het Netwerk Device

Nu je drivers werken en je eth0 en eth1 kan zien in ifconfig is het tijd om je interne netwerk in te gaan stellen. Ik neem aan dat je je interne netwerk op eth1 zet en je externe netwerk op eth0.

Je interne netwerk wordt een prive netwerk en zal daarom op een speciaal gereserveerd netwerk voor interne netwerken zijn: 192.168.1.0. Dit is een "private Class C network", in het geval dat je indruk wilt maken op je vrienden.

Eerst moeten we zeker weten dat netwerken aan staat. Verander de file /etc/sysconfig/network en weet zeker dat de volgende regels er in staan:

```
NETWORKING=yes
FORWARD_IPV4=yes
```

De eerste regel vertelt Linux dat we het netwerk device geactiveerd willen hebben als we opstarten. De tweede regel verteld Linux dat IP forwarding moet worden aangezet. Dit is nodig als we masquerading gaan configureren in Sectie 4.

Alle netwerk interface instellingen voor Red Hat en Red Hat afgeleiden staan in de files in de directory /etc/sysconfig/network-scripts. Ga naar de directory en maak een file ifcfg-eth1. Zet het volgende in die file:

```
DEVICE=eth1
IPADDR=192.168.1.1
ONBOOT=yes
```

Deze code verteld de netwerk scripts dat eth1 bij het booten moet worden geconfigureerd en dat ze het een vast Ip adres moeten geven. Activeer je netwerk met de nieuwe instellingen met het volgende commando: /etc/rc.d/init.d/network restart

3.2.2 De DHCP Server

Een DHCP server zal automatisch devices op je interne thuis netwerk Ip adressen geven. Dit is erg handig voor mensen met laptops: zij kunnen simpel hun machines in het netwerk pluggen en ze zijn gelijk goed geconfigureerd. Als je geen DHCP server wilt in je interne thuisnetwerk ga dan door naar de volgende sectie.

Eerst moet je kijken of je de DHCP server hebt geinstalleerd. Mount je Linux CD en installeer de `dhcp` RPM. Verander nu de `/etc/dhcpd.conf` file en zet het volgende (en alleen het volgende) er in:

```
subnet 192.168.1.0 netmask 255.255.255.0 {
  range 192.168.1.2 192.168.1.60;
  default-lease-time 86400;
  max-lease-time 86400;
  option routers 192.168.1.1;
  option ip-forwarding off;
  option broadcast-address 192.168.1.255;
  option subnet-mask 255.255.255.0;
}
```

Als je je Linux box gaat instellen als een caching domain name server, zet dan de volgende optie er ook bij:

```
option domain-name-servers 192.168.1.1;
```

Als je de buiten DNS adressen weet en als je je linux Box *niet* gaat gebruiken als een DNS server, zet er dan de volgende optie bij, waar x.x.x.x en y.y.y.y zijn de IP nummers van de DNS server:

```
option domain-name-servers x.x.x.x, y.y.y.y;
```

Als je een Samba file deling gaat draaien op je Linux box voor je Windows computer, zet er dan de volgende opties nog bij om je Linux box als de standaard Wins en browsing server te gebruiken:

```
option netbios-name-servers 192.168.1.1;
option netbios-dd-server 192.168.1.1;
option netbios-node-type 8;
option netbios-scope "";
```

Samba en WINS configureren is ver buiten beschouwing van dit document. Als je een link wilt, start met de *SMB HOWTO* en ga van daaruit verder.

Er zijn nog steeds een paar stappen. Verander de `/etc/rc.d/rc.local` file en voeg de volgende regels toe aan het einde:

```
# Set up the broadcast device to support DHCP
/sbin/route add -host 255.255.255.255 dev eth1
```

Windows DHCP clients hebben een speciaal broadcast adres nodig het DHCP antwoord, en dit commando forceert de Linux TCP/IP stack het te produceren.

De volgende stap de is de `/etc/rc.d/init.d/dhcpd` file `eth1` laten gebruiken als het standaard device. Verander de regel:

```
daemon /usr/sbin/dhcpd
```

Met:

```
daemon /usr/sbin/dhcpd eth1
```

OK, nu zijn we klaar om DHCP te starten. Start eerst de DHCP server met het commando: `/etc/rc.d/init.d/dhcpd start`. Voeg nu het speciale broadcast adres toe met `/sbin/route add -host 255.255.255.255 dev eth1`.

Tot slot, we moeten zeker weten dat de DHCP server start als we de computer opnieuw opstarten. Sommige RPM packages van de DHCP server hebben geen instructies om zeker te weten dat de server elke keer start, dus doen wij het met `chkconfig dhcpd on`.

Dit commando zorgt ervoor dat RedHat het dhcp opstart script toevoegt aan de verschillende runlevel directory's onder `/etc/rc.d`. In de runlevels 3 en 5 (multiuser console en multiuser X) wordt de DHCP server gestart. In de runlevels 0, 1 en 6 (shutdown, single user en reboot) wordt de DHCP server gestopt.

3.2.3 De Client Computers

Als je DHCP hebt ingesteld, is het configureren van je client computers erg simpel: Zet gewoon DHCP configuratie aan. Voor Windows computers, houd dit in het open van het "Control Panel" en de "Networking" optie kiezen. Vindt het "TCP/IP" protocol en doe "Configure" Zet "Configure TCP/IP address automatically" aan, sla de veranderingen op en reboot.

Voordat je reboot, kun je het volgende commando op je Linux box intypen: `tail -f /var/log/messages`. Dit houd je Linux systeem log continu in de gaten. Als alles goed gaat, als je je Windows computer her start, zie je een aanvraag voor een IP adres en je ziet de DHCP server antwoorden. Control-C sluit het `tail -f` commando af.

Als je DHCP niet hebt ingesteld, is het configureren nog steeds best simpel. Opnieuw open de "Networking" optie van het "Control Panel", en kies het configureren van het TCP/IP protocol. Je kan je client computers elk adres geven in het 192.168.1.0 netwerk behalve 192.168.1.0 (het netwerk adres), 192.168.1.255 (het broadcast adres) of 192.168.1.1 (je Linux server). Geef nooit twee computers het zelfde IP adres. Zet het "Gatewayädres op 192.168.1.1, zodat het uitgaande verkeer via je Linux gateway gaat.

De *IP Masquerading HOWTO* heeft erg gedetaileerde informatie over client configuratie in de *Configuration Section*.

3.2.4 De DNS Server

Je Linux box instellen als een cachins DNS server zal je surfsnelheid op het internet (een beetje) verhogen, omdat vaak gebruikte DNS adressen worden opgeslagen in je netwerk en moeten dan niet meer worden opgehaald van buiten af.

Als je interesse hebt in een volledige DNS server, is er een grote hoeveelheid aan complexiteit te leren. Er is een *DNS HOWTO* verkrijgbaar, en het boek *DNS and BIND* is een goede en omvattende papieren referentie.

Om je client machines te laten profiteren van de caching server, moeten ze Linux gateway gebruiken als de primaire DNS server. De DHCP directieven gegeven in sectie 3.2.2 is manier om het voor elkaar te krijgen. Als je je client computer met de hand configureerd, kun je de DNS configuratie in het zelfde menu doen als waar je je IP adres hebt ingesteld van de machine.

Om de DNS server te installeren, installeer je eerst de `bind` RPM, en daarna de `caching-nameserver` RPM. Nu ben je bijna klaar.

Geinstalleerd werkt de caching server goed, maar als je de IP adressen van de DNS server van je provider weet kan dit de snelheid verhogen. Dit stel je in door de `/etc/named.conf` file te veranderen en de volgende regels toe te voegen na de `directory` regel (waar x.x.x.x en y.y.y.y de primaire en secondary DNS server zijn):

```
forwarders { x.x.x.x; y.y.y.y; };
```

Deze verandering laat je DNS server eerst kijken bij je ISPs DNS servers voordat hij het internet helemaal oversteekt om te zoeken naar het gegeven adres. De server van de ISPs hebben vaak een grote cache aan DNS informatie en zij kunnen veel sneller antwoord geven dan andere servers.

OK, nu kunnen we de DNS server starten: `/etc/rc.d/init.d/named start`

3.2.5 Het binnen netwerk testen

Totdat we het buiten netwerk hebben ingesteld zal de DNS dienst niet werken (sinds hij moet communiceren met andere DNS servers op het internet), maar we kunnen de basis interne verbindingen testen met het `ping` programma.

Op een van je client computers, open een terminal (MSDOS) scherm, en type `ping 192.168.1.1`. Dit zend een pakketje naar je Linux computer op reguliere intervallen, en je Linux computer zal de packetjes terug zenden. Als de dingen goed werken, zou je packetjes terug moeten zien komen.

3.3 Het buiten netwerk configureren

Nu zijn we klaar om het buiten netwerk te configureren. Soms zal dit moeilijk zijn, dit hangt af van hoe goed je internet provider Linux ondersteunt. Als je problemen hebt is er een *ADSL mini-HOWTO* welke dingen gedetailleerd verteld over ADSL. Als ik een Kabel Modem HOWTO kan vinden zal ik die ook linken.

Het grootste probleem met buiten connecties is het *krijgen van een IP adres*. Sommige internet providers geven statische Ip adressen aan kabel en adsl gebruikers, en in dat geval is het configureren makkelijk. Hoewel, veel providers nu zijn overgestapt op dynamische configuratie via (je raad het) DHCP. Dit betekend dat je Linux computer een DHCP *server* is op je `eth1` interface en een DHCP *client* op je `eth0` interface.

Veel providers bieden hun diensten aan op niet standaard manier wat aanneemt dat hun klanten Windows gebruiken. Sommige van deze gevallen worden besproken op het einde van sectie 3.3.2.

3.3.1 Met een statisch IP

Als je internet provider je een statisch IP adres heeft gegeven, zit je goed. Eerst, maak een nieuwe interface configuratie file, `/etc/sysconfig/network-scripts/ifcfg-eth0` en zet er het volgende in:

```
DEVICE=eth0
IPADDR=x.x.x.x
```

```
NETMASK=y.y.y.y
ONBOOT=yes
```

Zet bij x.x.x.x en y.y.y.y de waarden die je internet provider je gegeven heeft. Verander nu de `/etc/resolv.conf` file en vul de volgende informatie in:

```
search provider_domain_here
nameserver n.n.n.n
nameserver m.m.m.m
```

Het provider_domain zou gegeven moeten zijn door je internet provider. Vul ook de primaire en secudaire DNS server in de n.n.n.n en m.m.m.m regels. Als je je Linux doos in hebt gesteld als een DNS server, kun je een regel toevoegen voor de andere nameservers met: `nameserver 127.0.0.1`. Dit zorgt ervoor dat je server eerst de caching server gebruikt voordat hij de DNS servers van de provider om DNS informatie vraagt.

3.3.2 Met DHCP

Als je internet provider DHCP configuratie gebruikt, moet je een nieuwe interface configuratie file maken, `/etc/sysconfig/network-scripts/ifcfg-eth0` en er het volgende in zetten:

`DEVICE=eth0`

`BOOTPROTO=dhcp`

`ONBOOT=yes`

Nu kijk je of de dhcpcd client deamon is geinstalleerd op je systeem. Ga naar je Linux CD en installeerd het `dhcpcd` RPM package.

Het is tijd om je nieuwe netwerk configuratie te testen. Gebruik gewoon het commando `/etc/rc.d/init.d/network restart`. Test nu de connectie naar buiten met ping. Ping een computer op het internet, zoals `www.yahoo.com` en kijk of er iets terug komt.

3.3.3 Vreemde en Afwijkende

Je situatie kan verschillend zijn met de erg simpele situatie hierboven beschreven. Hier zijn enkele korte opmerkingen op de verschillende moeilijkheden en links naar meer geautoriseerde bronnen en de adressen van die bronnen. Dank aan John Mellor voor het geven van de links en de aansporing om deze sectie toe te voegen.

PPP Over Ethernet (PPPoE) Veel ADSL providers (Bell Atlantic, bijvoorbeeld) staan er nu op dat hun nieuwe klanten verbinding maken met de dienst met het "PPP over Ethernet" protocol (PPPoE). Tot nu toe, geven ze een Windows client programma: niet erg bruikbaar voor Linux gebruikers. Gelukkig is PPPoE een simpel protocol en veel krachtsinspanningen zijn er om er Linux ondersteuning voor te krijgen, ze zijn allemaal in het vroege stadium.

- *PPPoE met Linux voor Bell Sympatico*
- PPPoE voor Linux voor Sympatico (*Algemene Info*) (*Linux Info*)

Stomme DHCP truukjes Een van de favoriete truuks van netwerk providers is hun dienst aan een unieke hostnaam binden, of zelfs een unieke netwerk kaart. Dit is vermoedelijk om je tegen te houden om verschillende computers in je ethernet poort met een hub (natuurlijk, met het gebruik van Linux en Masquerading krijg je het zelfde effect met betere veiligheid en de kabel maatschappij weet het niet eens!).

Als de provider je een hostnaam heeft gegeven en erop staat dat je je Windows box met die hostnaam instelt om hun dienst te gebruiken, dan moet je zeker weten dat je Linux box deze hostnaam zend als hij vraagt om een adres van de DHCP server.

De Red Hat DHCP client wordt aangeroepen als je het BOOTPROTO om dhcp insteld in de interface configuratie file, maar het wordt aangeroepen zonder referente naar een hostname. Om het programma aanteroepen met een hostname, in Red Hat 6.1, verander de `/etc/sysconfig/network` file en verander de regel:

```
HOSTNAME=
```

Naar dit:

```
HOSTNAME=your_isp_assigned_name
```

Dit zal niet werken in sommige Red Hat varianten. Als het niet werkt, kijk dan in het `/sbin/ifup` script en kijk of het het dhcpcd en pump programma aanroept met de -h $HOSTNAME optie. Als ze dat niet doen, voeg het dan toe, zodat de aanroep er als volgt uit ziet: `/sbin/dhcpcd -i $DEVICE -h $HOSTNAME` en `/sbin/pump -i $DEVICE -h $HOSTNAME`.

Road Runner De Road Runner kabel dienst heeft een speciaal login proces wat gedraait moet worden voordat de server gebruikt kan worden. Gelukkig is er een zeer gedetailleerde *Linux Road Runner HOWTO* verkrijgbaar.

3.3.4 Naar de netwerk intreden kijken.

Nu kun je je werk bewonderen. Type `ifconfig` om al je geconfigueerde devices te zien. Op mijn gateway computer ziet het er zo uit:

```
eth0  Link encap:Ethernet  HWaddr 00:60:67:4A:02:0A
      inet addr:24.65.182.43  Bcast:24.65.182.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:487167 errors:0 dropped:0 overruns:0 frame:0
      TX packets:467064 errors:0 dropped:0 overruns:0 carrier:0
      collisions:89 txqueuelen:100
      Interrupt:10 Base address:0xe400
eth1  Link encap:Ethernet  HWaddr 00:80:C8:D3:30:2C
      inet addr:192.168.1.1  Bcast:192.168.1.255  Mask:255.255.255.0
      UP BROADCAST RUNNING MULTICAST  MTU:1500 Metric:1
      RX packets:284112 errors:0 dropped:0 overruns:0 frame:1
      TX packets:311533 errors:0 dropped:0 overruns:0 carrier:0
      collisions:37938 txqueuelen:100
      Interrupt:5 Base address:0xe800
lo    Link encap:Local Loopback
      inet addr:127.0.0.1  Mask:255.0.0.0
      UP LOOPBACK RUNNING  MTU:3924  Metric:1
      RX packets:12598 errors:0 dropped:0 overruns:0 frame:0
      TX packets:12598 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
```

Zie dat het `eth0` interface een fantastisch buiten IP adres heeft en het `eth1` adres is een prive intern adres.

Je kan naar de netwerk routes kijken door het typen van het `route` commando. Op mijn gateway computer ziet het er zo uit:

```
Kernel IP routing table
Destination     Gateway      Genmask         Flags Metric Ref Use Iface
255.255.255.255 *            255.255.255.255 UH    0      0     0 eth1
192.168.1.0     *            255.255.255.0   U     0      0     0 eth1
24.65.182.0     *            255.255.255.0   U     0      0     0 eth0
127.0.0.0       *            255.0.0.0       U     0      0     0 lo
default         24.65.182.1  0.0.0.0         UG    0      0     0 eth0
```

Hier zien we dat het buiten netwerk is ingesteld en ook het binnen netwerk. Het locale device is ingesteld, het speciale broadcast adres is ingesteld, en de standaard route wijst naar de gateway van de internet provider. Perfect!

Nu je het buiten en binnen netwerk hebt. Alles wat nog nodig is is de deur tussen die twee openen. Eerst, moeten we zeker weten dat dat er geen monsters van buiten naar binnen komen.

3.4 Security

Een van de nadelen van het permanent online zijn met ADSL of Kabel is dat je computer wordt bloot gesteld aan potentiele security bedreigingen 24 uur per dag, 7 dagen in een week. Linux gebruiken als gateway verlaagt de risico's, omdat het alle andere computers verstopt: in zo verre dat de rest van het internet dat weet, alleen je Linux box is beschikbaar voor connecties. Dit betekent dat je netwerk alleen zo veilig is als je Linux box, dus nu geef ik een paar standaardtips om je computer veiliger te maken.

Eerst, moet je alle slechte mensen buiten sluiten. Om dit te doen, verander de file `/etc/hosts.deny` en weet zeker dat het er zo uit ziet:

```
#
# hosts.deny  This file describes the names of the hosts which are
#             *not* allowed to use the local INET services, as decided
#             by the '/usr/sbin/tcpd' server.
#
#             The portmap line is redundant, but it is left to remind you that
#             the new secure portmap uses hosts.deny and hosts.allow. In particular
#             you should know that NFS uses portmap!
ALL: ALL
```

Dit verteld de "TCP wrappers" – wat 95% van de inkomende verbindingen beheert – om alle verbindingen van alle computers af te wijzen. Dit is een erg goede regel! Maar, het houdt je binnen computers ook tegen verbinding te zoeken met je Linux computer, wat erg lastig is, dus we maken een uitzondering. Verander de file `/etc/hosts.allow` en weet zeker dat deze er zo uitziet:

```
#
# hosts.allow  This file describes the names of the hosts which are
```

```
#               allowed to use the local INET services, as decided
#               by the '/usr/sbin/tcpd' server.
#
ALL: 127.0.0.1
ALL: 192.168.1.
```

Dit verteld de "TCP wrappers" dat ze verbing naar alle diensten kunnen toestaan van het locale device (127.0.0.1) en van je thuis netwerk (192.168.1.).

Je hebt nu de monsters buiten gesloten, met een sterk hangslot. Als je versperringen en alarm systemen wilt instellen moet je veel gecompilceerder zijn. De *Security HOWTO* is een goede plek om te starten als je meer wilt leren over hoe je je Linux box veiliger moet maken.

4 Masquerading configureren

Ok! De voorbereidingen zijn voorbij, dit is waar de magie begint. IP masqueradingn is een van de echte magische diensten die Linux verstrekt. er zijn commerciele producten voor Windows welke het zelfde doen, maar niet zo efficient: een oude 386 kan gelukkig IP masqueradingn diensten verstrekken aan een heel gemiddeld groot kantoor, maar kan niet eens Windows 95 draaien, laat staan het masquerading pakket.

Linux heeft een extreem veelzijdige firewall mogelijkheid, en wij gaan het gebruiken in de simpelste en meeste grove manier gebruiken. Als je wilt leren om firewalls te maken als een expert, moet je de *Firewalling HOWTO* voor het begrijpen van de theorie lezen en de *IPChains HOWTO* voor instrucies voor de nieuwe `ipchains` firewall tool welke zit bij de Linux 2.2.X kernel (en bij uitbreiding Red Hat 6.X). Er is nu ook een erg goede *IP Masquerading HOWTO* verkrijgbaar welke meer details van masquerading bescrijft.

Simpel masquerading configuren is heel erg simpel als je interne en externe netwerk operationeel zijn. Verander de `/etc/rc.d/rc.local` file en voeg de volgende regels onderaan toe:

```
# 1) Flush de regel tabellen.
/sbin/ipchains -F input
/sbin/ipchains -F forward
/sbin/ipchains -F output
# 2) Stel de MASQ timing in en sta DHCP configuratie pakketjes toe.
/sbin/ipchains -M -S 7200 10 60
/sbin/ipchains -A input -j ACCEPT -i eth0 -s 0/0 68 -d 0/0 67 -p udp
# 3) Wijs alle forwarding pakketjes af behalve die van het lokale netwerk.
#    Masquerate die.
/sbin/ipchains -P forward DENY
/sbin/ipchains -A forward -s 192.168.1.0/24 -j MASQ
# 4) Laad forwarding modules voor speciale diensten.
/sbin/modprobe ip_masq_ftp
/sbin/modprobe ip_masq_raudio
```

De laatste twee regels voegen de kernel modules in om FTP en RealAudio te laten werken voor de computers in het binnen netwerk. Er zijn andere modules voor speciale diensten welke je kan invoegen als je ze nodig hebt:

- CUSeeMe (`/sbin/modprobe ip_masq_cuseeme`)

- Internet Relay Chat (`/sbin/modprobe ip_masq_irc`)
- Quake (`/sbin/modprobe ip_masq_quake`)
- VDOLive (`/sbin/modprobe ip_masq_vdolive`)

Nu ben je klaar om masquerading te proberen! Draai het `rc.local` script met het commando `/etc/rc.d/rc.local` en je bent klaar om te gaan! Ga zitten achter een van je andere computers en probeer om te surfen. Met een beetje geluk is nu alles alles kits.

5 Problemen

Er zijn een hele hoop dingen die fout kunnen gaan door het gebruik van een simpel document als dit, omdat er veel speciale gevallen zijn. De belangrijkst van mogelijke problemen blijven bij het configureren van het interne en externe netwerk device. Ik probeer antwoord te geven aan mensen met problemen, uitzoeken wat er fout is gegaan en links hieronder toevoegen zodat mensen met speciale problemen hulp kunnen vinden. Je kunt me bereiken op *pramsey@refractions.net*.

5.1 ICQ Werkt niet

Sommige delen van ICQ werken goed over masquerading. Andere delen werken helemaal niet goed. Er is een *beta kwaliteit ICQ module* in ontwikkeling, hoewel, welke adressen sommige (maar niet alle) van de gebreken van het draaien van ICQ over masquerading. De `README` file in de bron code distributie beschrijft hoe je de module moet compileren. Als je het hebt gecompileerd en geinstalleerd draai dan het commando `/sbin/modprobe ip_masq_icq`.